A

Architecture: (1) The design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a communications network. (2) The structure of an existing communications network, including the physical configuration, facilities, operational structure, operational procedures, and the data formats in use (MIL STD 188).

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [Source: ORD].

B

Base Waveform: A waveform software application that have been verified through JTeL, JITC and NSA for standards compliance, interoperability, and security requirements. Also see Waveform [Source: PMP]

Block: See Increment

C

Centers of excellence: Institutions possessing special knowledge or expertise in a particular area of concern and incorporated into the collaborative environment to facilitate development of the products supporting SJFHQ and JTF functions and operations, e.g., academia, industry, banking. [Source: JFCOM glossary]

Channel: An independent operational capability providing a waveform capability. A channel is a single processing path within a single JTR Set that supports all functionality required by a specific waveform. A channel may involve half-duplex or full-duplex operation. [Source: ORD]

Cluster: Within the JTRS program, a grouping of radio procurements based on similarity of requirements and required fielding schedules. [Source: PMP]

Common Operating Environment (COE): The collection of standards, specifications, and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces (APIs), runtime environment definitions, reference implementations, and methodology that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product (DII COE I&RTS).

Configuration Management: It identifies, controls, accounts for, and audits all changes made to a site or information system during its design, development, and operational life cycle (DoD CIO Guidance IA6-8510 IA).

Core Performance Requirements: The JTR Set core performance requirements are the common baseline functionality that each JTR Set will have to provide basic interoperability for the warfighters. [Source: ORD]

D

Data Rates: The aggregate rates at which data pass a point in the transmission path of a system. LOW, MEDIUM and HIGH Data rates are further defined in applicable MIL STDs for applicable waveform and system usages. [Source: ORD]

E

Evolutionary Acquisition: An acquisition strategy that defines, develops, produces or acquires, and fields an initial hardware or software increment (or block) of operational capability. It is based on technologies demonstrated in relevant environments, time-phased requirements, and demonstrated manufacturing or software deployment capabilities. These capabilities can be provided in a shorter period of time, followed by subsequent increments of capability over time that accommodate improved technology and allowing for full and adaptable systems over time. Each increment willmeet a militarily useful capability specified by the user (i.e., at least the thresholds set by the user for that increment); however, the first increment may represent only 60% to 80% of the desired final capability.

There are two basic approaches to evolutionary acquisition. In one approach the ultimate functionality can be defined at the beginning of the program, with the content of each deployable increment determined by the maturation of key technologies. In the second approach the ultimate functionality cannot be defined at the beginning of the program, and each increment of capability is defined by the maturation of the technologies matched with the evolving needs of the user.
[Source: USD ATL memo of April 2002]

F

Flexibility in Form Factor: Relates to the ability of a set to be adapted into configurations for integration into the various platforms. [Source: ORD]

G

Gateway: A gateway in a communications network is a network node equipped for interfacing with another network that uses different protocols. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires that mutually acceptable administrative procedures be established

between the two networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions. A multi-channel JTR set includes inter-network gateway services between its channels or networks. [Source: ORD]

Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:
(1) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software and services.
(2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software and services.
(3) Processes data or information for use by other equipment, software and services.
[Source: memo from PDUSD (AT&L); PASD (C3I)/CIO; VD J-6 (may '01)

H

Hardware Configuration: A set of interconnected equipment forming a system. The hardware of a particular JTR set will be physically configured for operating specific waveforms to meet the needs of specific platforms. [Source: PMP]

I

Increment or Block: A militarily useful and supportable operational capability that can be effectively developed, produced or acquired, deployed, and sustained. Each increment of capability will have its own set of thresholds and objectives set by the user.
[Source: Memo from USD ATL of April 2002]

Information Assurance: Information Operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. [Source: ORD]

Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. [Source: DoD Dictionary]

Information Superiority: That degree of dominance in the information domain which permits the conduct of operations without effective opposition. See also information operations. [Source: DoD Dictionary]

Information Superiority: The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information Superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives [Source: JV 2010]

Information Warfare: Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. [Source: DoD Dictionary]

Instantiation: An operator action to select a software waveform from a radio set's stored waveform and activate the waveform on a JTR set hardware channel. [Source: ORD]

Inter-Networking: Inter-networking is the process of inter-connecting two or more individual networks to facilitate communications between nodes of the inter-connected networks. Each network may be distinct, with its own addresses, internal protocols, access methods, and administration. Individual networks connected to form a JTR inter-network will share the same general operating mode, i.e. voice, data, or video. [Source: ORD]

Integrity: Integrity is the property that data, systems, services, and other controlled resources have not been altered or destroyed in an unauthorized manner. It is the quality of an information system (IS) that reflects the logical correctness and reliability of the operating systems and the logical completeness of the hardware and software that implement the protection mechanisms. [Source: ORD]

Interoperability: The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. For example, interoperability could be established between a SINCGARS voice net and another system voice net through a transparent interface of a JTR set operating simultaneously in both nets. [Source: PMP]

Interoperability Categories: Wireless interoperability can generally be achieved by the use of one of the following four categories:

1) Same Radio (Direct interoperability, across different domains or among different equipment. Example: SINCGARS among ground forces, or JTR System among all services, etc.).
2) Common Waveform (Direct interoperability, across different domains or among different equipment. Example:

SINCGARS waveform between SINCGARS and JTR System radio sets).
3) Gateways & Relays (Indirect interoperability, and/or for range extension (usually automatic), may include conversion of frequencies, modes, protocols, cryptographic cover, etc., and may be in real or non-real-time. Example: JTR set employed to "patch" a SINCGARS net to a HAVE QUICK net. See also "gateway" and "route and retransmission".)
4) Equipment Duplication (Indirect interoperability (usually manual), using multiple "stovepipe" radios, may be employed due to time, operational, security, or other constraints, and often the first (and usually inefficient) choice. Example: stack of non-interoperable radios with a very busy operator).
[Source: ORD]

J

Joint Tactical Radio (JTR) Set: A JTR set is integrated on a user's platform as a completely functional configuration of radio communications hardware and software that provides the full range of JTR System services required by the user system. The JTR Set may include one or more operating components. A JTR set does not include the user's host system computer, but does provide all aspects of radio communications and network services intended for the user's host system. A JTR set includes, but is not limited to such items as receiver-transmitters; microphones and speakers, antennae; power amplifiers; batteries for dismounted sets; interconnecting cables; platform installation kits, routers and other networking components; etc. JTR set examples:
Set 1. Hand-held 1-channel/1 mode HF voice radio, power, and antenna.
Set 2. Hand-held 1-channel/1 mode VHF voice radio, power, and antenna.
Set 3. Dismounted 2-channels/2modes VHF voice/VHF data radio, power, and antenna.
Set 4. Vehicular or Aviation 3-channels/2modes VHF voice/VHF data/UHF/data radio, inter-networking components, power, antenna, platform installation kit, etc.
Set 5. A 6 channels/2modes JTR Set, designed for interim use during the transition from legacy radios to JTR Set, could be comprised of 1 software-defined radio programmed for 3 channels (e.g. SINCGARS voice net 1, SINCGARS voice net 2, and HAVEQUICK voice net); 3 adjunct legacy radios (e.g. JTIDS, EPLRS and UHF DAMA/DASA); and the means to inter-connect the channels as required for inter-networking.
[Source: ORD]

JTR System (JTRS): JTRS is a generic reference to the system that encompasses the aggregate of all aspects and components (including JTR sets) that constitute and enable the installation, operation and maintenance of the JTRS communications architecture. Unless explicitly stated otherwise, JTRS is a collective term that refers to the entire system. [Source: PMP]

JTRS Certification: A process of independent test and evaluation that assures that a waveform or other JTRS component is compliant with the Software Communications Architecture; compliant with security requirements; is portable to other JTR sets; conforms with appropriate standards; and is interoperable with legacy systems where appropriate. Full JTRS Certification is achieved only after at least one Service has ported the waveform to its JTR set and successfully completed the appropriate Security Verification Test (NSA) and JTIC Conformance and Interoperability Test.
[Source: JTRS PMP p. 22]

JTRS Compliance: Verification, through testing and analysis, that each JTRS product (resulting from a specific JTRS acquisition) addresses the joint goals and objectives of the JTRS program, and that all technical and operational requirements set forth in the specific Cluster and/or Waveform acquisition procurements have been met. Since no particular radio product is guaranteed/required (or tested) to meet the JTRS ORD requirements except ones that are part of a JTRS acquisition, JTRS compliance is inherently tied to a JTRS acquisition.

L

Line Replaceable Unit: A box or assembly that is installed or removed from the JTR set by the operator/maintainer as a single serviceable entity. [Source: ORD]

Local: In context of JTR System control and management, by means of integral, attached, on board, or other proximal means, such as front panel, cockpit display, or similar nearby control device. [Source: ORD]

M

Modular/Module: Modular pertains to a design concept in which interchangeable units are used to create a functional product. A module is an interchangeable subassembly that constitutes part of a larger device or system. A modular system is constructed with standardized units or dimensions for flexibility and variety in operational use and cost-effective modifications to either hardware or software. Modularity may be scaled to any system functional or design level that promotes desired efficiency. [Source: ORD]

Mobile User Objective System: The Mobile User Objective System (MUOS) will be a system of systems supporting narrowband (64 kbps and below) beyond line-of-sight connectivity for worldwide mobile and fixed-site terminals. MUOS does not include user hand-held terminals. It provides range extension for those terminals. [Source: ORD]

Multi-Band Operation: Multi-band refers to operations in the frequency spectrum between limits of defined frequency bands for two or more channels, radios, or networks. Multi-band JTR operations may use several different transmission channels (frequencies), waveforms, or networks to pass information between user terminals. [Source: ORD]

Multi-mode Operation: Multi-mode operation refers to a capability to operate more than one mode on a channel, radio, or system. Multi-mode JTR sets will operate to exchange information using voice, video, or data modes. [Source: ORD]

Multilevel Security: Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. [Source: ORD]

Multiple Single Levels of Security: A processing system in which information at different levels of classification is processed, but the information is not combined in any way. [Source: ORD]

N

Network Bridge: A device that links or routes signal from one network to another. [Source: ORD]

Network Centric Warfare: An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace. [Source: book, Network Centric Warfare]

Node: A general term used to describe either a terminal connection point common to two or more branches of a network; a switch forming a network backbone; patching and control facilities; or technical control facilities. [Source: ORD]

O

Open System: An open system has characteristics that comply with specified, publicly maintained, readily available standards. [Source: ORD]

Open System Architecture: Open systems architecture is non-proprietary. Open systems architecture is the layered hierarchical structure, configuration, or model of a communications or distributed data processing system that:

(**a**) Enables system description, design, development, installation, operation, improvement, and maintenance to be performed at a given layer or layers in the hierarchical structure.
(**b**) Allows each layer to provide a set of accessible functions that can be controlled and used by the functions in the layer above it.
(**c**) Enables each layer to be implemented without affecting implementation of other layers.
(**d**) Allows the alteration of system performance by the modification of one or more layers without altering the existing equipment, procedures, and protocols at the remaining layers.
[Source: ORD]

Over-the-Air Rekeying: Changing traffic encryption key or transmission security key in remote crypto-equipment by sending the new key directly to the remote crypto-equipment over the communications path it secures. [Source: ORD]

Over-the-Air-Transfer: Electric distribution of a key without changing the traffic encryption key used on the secured communications path over which the transfer is accomplished. [Source: ORD]

Over-the-Air-Zeroization: Effecting a zeroization in remote crypto-equipment by sending an authenticated "zeroize" command directly to the remote crypto-equipment over the communications path it secures. [Source: ORD]

P

Programmable: Pertains to a device that accepts instructions (usually via software) that alter its basic functions.

Protocol: A formal set of conventions governing the format and control of interaction among communication functional units. In layered communications system architecture, a protocol is a formal set of procedures that are adopted to facilitate functional inter-operation within the layered hierarchy. [Source: ORD]

Protocol Converter: A functional unit that uses a specified algorithm to translate a bit-stream from one protocol to another protocol to enable inter-operation between the two using systems. [Source: ORD]

Protocol Translator: In a communications system, a protocol translator is the collection of hardware, software, firmware, or any combination of these that is required or used to convert the protocols used in one network to those used in another network (e.g., Link 16 VMF to 188-220). Also see Gateway. [Source: ORD]

R

Remote: In the context of JTR System control and management, remote refers to a means of non-integral, detached, or other distal means, such as remote control panel, JTR System network management system, or similar distant control device, normally linked to the JTR set by wired, wireless or optical means. [Source: ORD]

Router and Retransmitter: A system designed to automatically pass user information from a channel operating on one medium to a channel operating on the same or another medium. Within a multi-channel radio set, routing and retransmission may occur between any input channel and any output channel that the set operates using the same mode of operation (voice, data, or video). Within a network, information may flow between two nodes that do not share a common channel by routing the data through another, multi-channel node that operates on both channels used by the source and destination nodes. A router and retransmitter is differentiated from a data forwarder in that it does not perform any data translation functions. With a router and retransmitter there is no manipulation or conversion of the data stream, and the original message header and contents/data elements remain intact. (JTDLMP)

Route and Retransmission: (Previously stated as Cross-banding) To route and retransmit is the capability to automatically pass user information from a channel operating on one frequency band to a channel operating on another frequency band. Within a multi-channel radio

set, routing and retransmission may occur between any input channel and any output channel that the set operates using the same mode of operation (voice, data, or video). Within a network, information may flow between two nodes that do not share a common channel by routing the data through a multi-channel node that operates on both channels used by the source and destination nodes. For example, in a JTR set operating the data mode simultaneously in two SINCGARS data nets and one EPLRS net, routing and retransmission of data flow can be accomplished between source nodes of one net and destination nodes of one or both other nets. Routing and retransmission in the JTR System may include use of multi-link operations. [Source: ORD]

S

SCA Compliance: Verification, through testing and analysis, that the specific waveform application and/or JTRS set and associated software have been implemented properly (i.e., in accordance with the current SCA and applicable annexes). SCA compliance refers to developing products in accordance with the SCA standard. SCA compliance is not synonymous with JTRS Compliance: a particular product can be SCA compliant, yet not meet any particular set of JTRS user requirements.

SCA Certification: Aprocess whereby a specific JTRS product is certified, such that the standard SCA compliance testing has been performed properly and with successful results; and that the waveform application and/or JTRS set has been implemented properly in accordance with the current SCA release. To achieve SCA certification requires that a waveform or JTRS set meet the following requirements:
- the waveform application or JTRS set must conform to all applicable interfaces and requirements set forth in the current SCA
- the developer must provide rationale/analysis and results of in-house execution of SCA compliance testing to demonstrate SCA compliance
- the waveform application must successfully pass all JPO standardized SCA compliance testing (using applicable JPO test requirements, JPO test procedures, and JPO developed test tools)

Scaleable System Design: A scaleable system design provides graduated levels of service or capabilities to fit various user needs. *The degree to which a system may be scalable is related to the degree to which the system components are modularized.* [Source: ORD]

Seamless: A condition that exists in a communications network whereby connectivity and throughput is accomplished without manual intervention. [Source: ORD]

Small Form Fit: In the context of a JTR set, a small form fit is a small lightweight radio transceiver communications device (e.g., card, module, subsystem, etc.) dedicated to performing radio transport functions that can be integrated into warfighter equipment, munitions, and sensors. [Source: ORD]

Software Communications Architecture: An architecture framework in that it is precise in areas where reusability is affected and is general in other areas so that unique requirements of implementation determine the specific application of the architecture. The Software Communication Architecture defines the hardware and software at different levels of detail to allow the broadest reusability and portability of components. [Source: ORD]

Software Defined Radio: A collection of hardware and software technologies that enable reconfigurable system architectures for wireless networks and user terminals. SDR provides an efficient and comparatively inexpensive solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades. As such, SDR can really be considered an enabling technology that is applicable across a wide range of areas within the wireless industry.
SDR enabled devices and equipment can be dynamically programmed in software to reconfigure the characteristics of the equipment. The same piece of "hardware" can be modified to perform different functions at different times…. SDR provides the user with a single piece of scalable hardware that is at once compatible at a global scale and robust enough to deliver a "pay as you go" feature set.
SDRs provide software control of a variety of modulation techniques, wide-band or narrow-band operation, communications security functions, and waveform requirements of current and evolving standards over a broad frequency range. [Source: SDR Forum website]

Spiral Development: An iterative process for developing a defined set of capabilities within one increment. This process provides the opportunity for interaction between the user, tester, and developer. In this process, the requirements are refined through experimentation and risk management, there is continuous feedback, and the user is provided the best capability within the increment. Each increment may include a number of spirals. Spiral development implements evolutionary acquisition.
[Source: USD ALT Memo of April 2002]

Spectrum Supportability: The assurance that the necessary frequencies and bandwidth are available to military systems in order to maintain effective interoperability in the operational electromagnetic environment. It includes spectrum certification, host nation coordination, frequency assignment, and electromagnetic compatibility. [Source: NCES Study Plan]

T

Tactical Communications System: A tactical communications system is used within or in direct support of tactical forces and is designed to meet the requirements of changing tactical situations and varying environmental conditions. It provides securable communications (e.g. voice, data, and video) among mobile users to facilitate command and control of tactical forces. A tactical communications system usually requires extremely short installation times in order to meet the requirements of frequent relocation. [Source: ORD]

Transformation: Transformation is a continuing process that is meant to create or anticipate the future. Transformation deals with the co-evolution of concepts, processes, organizations and technology to create new sources of power and yield profound and sustained increases in military competitive advantage. Transformation identifies, leverages and creates new underlying principles in the way things are done.
[Source: Office of Force Transformation-provided background paper and reviewed abstracted definition]

Transmission Security (TRANSEC): A component of COMSEC resulting from the application of measures taken to protect transmissions from interception and exploitation by means other than cryptanalysis (Cryptanalysis is defined as "Operations performed in converting encrypted

messages to plain text without initial knowledge the crypto-algorithm and /or key employed in the encryption.). Transmission security is the protection of the communications paths against attack. Defensive measures include anti-jam, low probability of detection, low probability of intercept, spread spectrum techniques such as frequency hopping and direct sequence spreading, and protected distribution. [Source: ORD]

Transparent Interface: A transparent interface allows the connection and operation of two or more systems, subsystems, or equipment without modification of characteristics or operational procedures on either side of the interface. *For example, a JTR set operating in a SINCGARS data net on one channel and an EPLRS data net on a second channel will provide the means for a transparent interface between the two nets. Thus, nodes in the SINCGARS net and nodes in the EPLRS net can transfer data between each other through the JTR set with neither user being aware of the path or means that enabled the transfer.* [Source: ORD]

V

Virtual JTR Intern-Network: A virtual JTR inter-network provides virtual circuits using the facilities of two or more real networks. Each type of JTR inter-network (voice, data or video) is a virtual network that uses real networks linked together by JTR sets. [Source: ORD]

W

Waveform: A waveform is the representation of a signal as a plot of amplitude versus time. In general usage, the term waveform refers to a known set of characteristics, e.g. SINCGARS or EPLRS "waveforms". In JTR System usage, the term waveform is used to describe the entire set of radio functions that occur from the user input to the RF output and vice versa. A JTR System "waveform" is implemented as a re-useable, portable, executable software application that is independent of the JTR System operating system, middleware, and hardware. [Source: ORD]

Waveform Conformance Testing: Testing process that determines if the waveform meets the requirements of military standards and waveform specifications. [Source: PMP]

Wide-Band: A wide band circuit may have a bandwidth wider than normal for the type of circuit, frequency of operation, or type of modulation. In common usage, "wide-band" refers to a high capacity for information transfer. In JTR System usage, wide-band refers to a networked radio waveform that has a node-to-node capacity for information transfer of 512 Kbps or greater. [Source: ORD]

Z

Zeroization: Removal or elimination of all RED keys and erasure of all classified data resident in unencrypted form. [Source: ORD]